SUBSCRIBER AUTHENTICATION IN A MOBILE COMMUNICATIONS SYSTEM

Patent number:	JP11513853 (T)
Publication date:	1999-11-24
Inventor(s):	
Applicant(s):	
Classification:	
- international:	*H04L9/32; H04W12/06;* H04L9/32; H04W12/00; (IPC1-7): H04L9/32; H04Q7/38
- european:	H04L9/32A; H04Q7/38A; H04W12/06
Application number:	JP19960515546T 19961016
Priority number(s):	WO1996FI00543 19961016; US19950544199 19951017

Abstract not available for JP 11513853 (T)
Abstract of correspondent: **WO 9715161 (A1)**
Translate this text

An authentication in a GSM based mobile comunications system relies on a challenge and response principle. A 32-bit Signed Response (SRES) parameter is calculated by A3 algorithm from a 128-bit Random Number (RAND) and a 128-bit Authentication Key Ki in a mobile station and in an authentication center, and the SRES values are compared. A CAVE algorithm having a 152-bit input parameter and an 18-bit output parameter is employed as the A3 algorithm. Paramater adaptation functions are provided between the input parameter of the CAVE algorithm and the GSM type input parameters, namely the random number RAND and the authentication key Ki, as well as between the output parameter of the CAVE algorithm and the GSM output parameter, namely the signed response SRES.

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号

特表平11－513853

(43)公表日　平成11年(1999)11月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ

審査請求　未請求　　予備審査請求　有　　（全 30 頁）

(21)出願番号　特願平9－515546
(86)（22)出願日　平成８年(1996)10月16日
(85)翻訳文提出日　平成10年(1998)４月15日
(86)国際出願番号　ＰＣＴ／ＦＩ９６／００５４３
(87)国際公開番号　ＷＯ９７／１５１６１
(87)国際公開日　平成９年(1997)４月24日
(31)優先権主張番号　０８／５４４，１９９
(32)優先日　1995年10月17日
(33)優先権主張国　米国（ＵＳ）

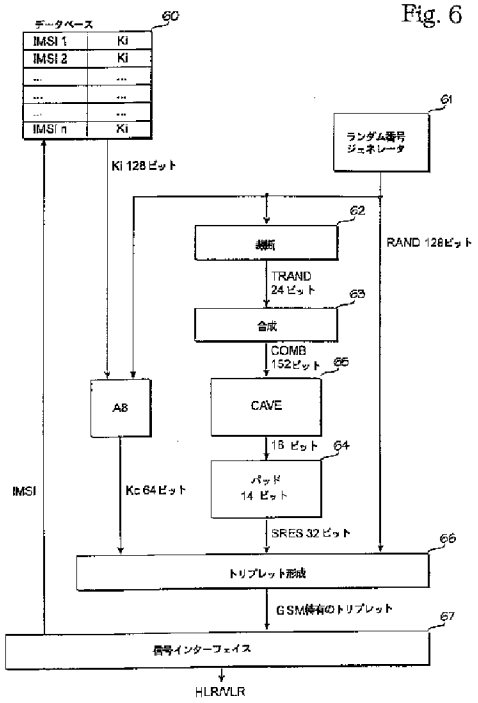
(71)出願人　ノキア　テレコミュニカシオンス　オサケ　ユキチュア
フィンランド　エフイーエン－02150　エスプー　ケイララーデンティエ　４
(72)発明者　ムルト　ユハーニ
アメリカ合衆国　テキサス州　75019　コッペル　スワロウ　ドライヴ　758
(74)代理人　弁理士　中村　稔　（外６名）

最終頁に続く

(54)【発明の名称】　移動通信システムにおける加入者確証

(57)【要約】
ＧＳＭベースの移動通信システムにおける確証は、チャレンジ・アンド・レスポンスの原理に基づいている。移動ステーション及び確証センターにおいて１２８ビットのランダム番号（ＲＡＮＤ）及び１２８ビットの確証キー（Ｋｉ）からＡ３アルゴリズムにより３２ビットの符号応答（ＳＲＥＳ）パラメータが計算され、そしてＳＲＥＳ値が比較される。１５２ビットの入力パラメータ及び１８ビットの出力パラメータを有するＣＡＶＥアルゴリズムが、Ａ３アルゴリズムとして使用される。ＣＡＶＥアルゴリズムの入力パラメータと、ＧＳＭ型の入力パラメータ、即ちランダム番号ＲＡＮＤ及び確証キーＫｉとの間、及びＣＡＶＥアルゴリズムの出力パラメータと、ＧＳＭの出力パラメータ、即ち符号応答ＳＲＥＳとの間に、パラメータ適応機能が与えられる。

Fig. 6



【特許請求の範囲】

１．移動通信ネットワークのための確証センターにおいて、

上記移動通信ネットワークの各加入者のための確証キーを記憶するデータベースを備え、上記確証キーは、暗号キー及び確証応答パラメータを計算するための入力パラメータであって、第１の確証手順に必要なフォーマットにあり、

更に、ランダム番号のソースを備え、このランダム番号は、暗号キー及び確証応答パラメータを計算するための別の入力パラメータであって、上記第１の確証手順に必要なフォーマットにあり、

更に、上記データベースからの確証キー及び上記ランダム番号のソースからのランダム番号を入力パラメータとして有し、そして上記第１の確証手順に基づくフォーマットで暗号キーを出力する暗号キー計算ユニットと、

単一入力パラメータを必要とし、そして上記第１の確証手順に基づく確証応答パラメータのフォーマット以外のフォーマットで確証応答パラメータを出力する確証応答パラメータ計算ユニットと、

入力パラメータとしての上記確証キー及び上記ランダム番号に応答して、上記単一入力パラメータを上記確証応答計算ユニットに与えるための第１の適応ユニットと、

上記確証応答パラメータ計算ユニットにより出力される上記確証応答パラメータに応答して、上記第１の確証手順に基づく確証応答パラメータを与えるための第２の適応ユニットと、

を備えたことを特徴とする確証センター。

２．移動ステーションの確証パラメータ処理ユニットにおいて、

上記移動ステーションを使用する移動加入者のための確証キーを記憶するメモリを備え、上記確証キーは、暗号キー及び確証応答パラメータを計算するための入力パラメータであって、第１の確証手順に必要なフォーマットにあり、

更に、ランダム番号のソースを備え、このランダム番号は、暗号キー及び確証応答パラメータを計算するための別の入力パラメータであって、上記第１の確証手順に必要なフォーマットにあり、

更に、上記データベースからの確証キー及び上記ランダム番号のソースから

のランダム番号を入力パラメータとして有し、そして上記第１の確証手順に基づくフォーマットで暗号キーを出力する暗号キー計算ユニットと、

単一入力パラメータを必要とし、そして上記第１の確証手順に基づく確証応答パラメータのフォーマット以外のフォーマットで確証応答パラメータを出力する確証応答パラメータ計算ユニットと、

入力パラメータとしての上記確証キー及び上記ランダム番号に応答して、上記単一入力パラメータを上記確証応答計算ユニットに与えるための第１の適応ユニットと、

上記確証応答パラメータ計算ユニットにより出力される上記確証応答パラメータに応答して、上記第１の確証手順に基づく確証応答パラメータを与えるための第２の適応ユニットと、

を備えたことを特徴とする確証パラメータ処理ユニット。

３．第１の確証応答計算方法と共に使用されるよう意図された確証手順を使用し；

上記第１の確証応答計算方法に代わって第２の確証応答計算方法を使用し；

上記第１の確証応答計算方法には適合するが上記第２の確証応答計算方法には適合しない確証キーを上記移動通信ネットワークの各加入者ごとに与え；

上記第１の確証応答計算方法には適合するが上記第２の確証応答計算方法には適合しないランダム番号を発生し；

上記確証キー及び上記ランダム番号から上記第２の確証応答計算方法に適合する入力パラメータを導出し；

上記移動通信ネットワークに使用される上記確証手順の確証応答フォーマットに適合しない確証応答を上記第２の確証応答計算方法により計算し；

この確証応答を上記確証手順の確証応答フォーマットに適合するフォーマットに変更し；そして

上記確証応答を上記確証手順に適合する上記フォーマットで移動通信ネットワークにおいて転送して記憶する；

という段階を備えたことを特徴とする移動通信ネットワークのための確証方法。

４．ＧＳＭをベースとする確証応答計算方法と共に使用されるよう意図されたＧＳＭをベースとする確証手順を使用し、上記ＧＳＭをベースとする確証応答

計算方法は、１２８ビットのランダム番号ＲＡＮＤ及びＮビットの確証キーＫｉを入力パラメータとして含むと共に、３２ビットの符号応答ＳＲＥＳを出力パラメータとして含み、Ｎは、正の整数であり；

上記ＧＳＭをベースとする確証応答計算方法に代わる確証応答計算方法としてＣＡＶＥ計算方法を使用し、このＣＡＶＥ方法は、１５２ビットの入力パラメータ及び１８ビットの出力パラメータを含み；

移動通信ネットワークの各加入者に対して上記ＮビットのＫｉの独特の値を与え；

Ｋｉの上記値を確証センターのデータベースに記憶し；

上記移動加入者の１人に対し上記ＳＲＥＳを与えるための要求を受け取り；

上記移動加入者の上記１人の上記ＮビットのＫｉを上記データベースから検索し；

上記１２８ビットのＲＡＮＤを発生し；

上記ＮビットのＫｉ及び１２８ビットのＲＡＮＤから上記１５２ビットの入力パラメータを導出し；

上記ＣＡＶＥ計算方法により上記１８ビット出力パラメータを計算し；

上記１８ビット出力パラメータに付加的な１４ビットをパッドして、上記３２ビットのＳＲＥＳを得；そして

上記ＧＳＭをベースとする確証手順に基づき上記ＧＳＭをベースとする移動通信ネットワークにおいて上記３２ビットＳＲＥＳを転送しそして記憶する；

という段階を備えたことを特徴とするＧＳＭをベースとする移動通信ネットワークのための確証方法。

５．上記導出段階は、

上記１２８ビットのＲＡＮＤを（１５２－Ｎ）ビットの裁断されたＲＡＮＤへと裁断し、Ｎは、１２８以下の整数であり、そして

上記（１５２－Ｎ）ビットの裁断されたＲＡＮＤを上記ＮビットのＫｉと合

成して、上記１５２ビットの入力パラメータを得る、

という段階を含む請求項４に記載の方法。

６．ＧＳＭをベースとする確証応答計算方法と共に使用されるよう意図された

ＧＳＭをベースとする確証手順を使用し、上記ＧＳＭをベースとする確証応答計算方法は、１２８ビットのランダム番号ＲＡＮＤ及びＮビットの確証キーＫｉを入力パラメータとして含むと共に、３２ビットの符号応答ＳＲＥＳを出力パラメータとして含み、Ｎは、正の整数であり；

上記ＧＳＭをベースとする確証応答計算方法に代わる確証応答計算方法としてＣＡＶＥ計算方法を使用し、このＣＡＶＥ方法は、１５２ビットの入力パラメータ及び１８ビットの出力パラメータを含み；

移動加入者に対して与えられた上記ＮビットのＫｉの独特の値を移動ステーションのメモリに記憶し；

上記１２８ビットのＲＡＮＤを含む確証要求を上記移動ステーションによりベースステーションから受け取り；

上記ＮビットのＫｉを上記メモリから検索し；

上記ＮビットのＫｉ及び１２８ビットのＲＡＮＤから上記１５２ビットの入力パラメータを導出し；

上記ＣＡＶＥ計算方法により上記１８ビット出力パラメータを計算し；

上記１８ビット出力パラメータに付加的な１４ビットをパッドして、上記３２ビットのＳＲＥＳを得；そして

上記３２ビットＳＲＥＳを上記ベースステーションへ送信する；

という段階を備えたことを特徴とするＧＳＭをベースとする移動通信ネットワークのための確証方法。

７．上記導出段階は、

上記１２８ビットのＲＡＮＤを（１５２－Ｎ）ビットの裁断されたＲＡＮＤへと裁断し、Ｎは、１２８以下の整数であり、そして

上記（１５２－Ｎ）ビットの裁断されたＲＡＮＤを上記ＮビットのＫｉと合成して、上記１５２ビットの入力パラメータを得る、

という段階を含む請求項６に記載の方法。

８．移動通信システムのための確証パラメータ計算ユニットにおいて、

１５２ビットの入力パラメータを受け取る第１入力と、１８ビットの出力パラメータを出力する出力とを有するＣＡＶＥアルゴリズム計算器と、

１２８ビットのランダム番号ＲＡＮＤを受け取る第１入力と、正の整数をＮとすれば、Ｎビットの確証キーＫｉを受け取る第２入力と、このＮビットのＫｉ及び１２８ビットのＲＡＮＤから導出された上記１５２ビットの入力パラメータを上記ＣＡＶＥアルゴリズム計算器の上記入力へ出力するための出力とを有する第１アダプタと、

上記ＣＡＶＥアルゴリズム計算器の１８ビット出力パラメータを受け取る入力と、３２ビットの符号応答ＳＲＥＳを出力する出力とを有する第２アダプタとを備え、上記Ｋｉ、ＲＡＮＤ及びＳＲＥＳは、ＧＳＭベースの確証パラメータであることを特徴とする確証パラメータ計算ユニット。

【発明の詳細な説明】

移動通信システムにおける加入者確証

発明の分野

本発明は、移動通信ネットワークのセキュリティ機能に係り、より詳細には、移動通信ネットワークにおいて加入者の確証を得ることに係る。

先行技術の説明

全てのテレコミュニケーションネットワークにおいて、ユーザ及びネットワークオペレータの両方を第三者の不所望な侵入に対してできるだけ保護しなければならない。従って、ネットワークには、多数の種類のセキュリティ機能が必要となる。ネットワークセキュリティの重要な観点は、１）ネットワークが搬送する情報の保護と、２）ネットワークのユーザの確証及びアクセス制御である。情報を保護するためのほとんどのセキュリティ機構は、ある形態の暗号化であり、それに留まり勝ちである。確証は、送って来るように請求されたソースから情報が確実に送られるように試みる手段である。これは、一般に、パスワード及びキーに基づいている。アクセス権は、送信媒体を経て送信及び／又は受信する能力に関して指定される。又、アクセス機構も、一般に、ある形態のパスワード又はキーに基づいている。

移動加入者への送信に無線通信が使用されるために、公衆地上移動ネットワーク（ＰＬＭＮ）のような無線アクセスネットワークは、特に、許可のないユーザによるリソースの誤用や、無線経路上で交換される情報の盗み聞きを感知する。これは、ユーザ又はオペレータの装置を変造せずに、どこからでも無線信号を聞いたり送信したりできることによるものである。ＰＬＭＮは、通常のテレコミュニケーションネットワークよりも高いレベルのセキュリティを必要とすることが明らかである。

ＧＳＭ（移動通信用のグローバルシステム）として知られているパン・ヨーロピアンデジタルセルラー無線は、機密性の高い確証システムを含んでいる。これは、いわゆるチャレンジ・アンド・レスポンスの原理に基づくものである。加入時に、加入者確証キー（Ｋｉ）と称する機密番号が、国際移動加入者認識（ＩＭＳＩ）と共に加入者に割り当てられる。この加入者確証キーＫｉは、加入

者のホーム位置レジスタ（ＨＬＲ）に関連するか又はそれにリンクされた確証センター（ＡＵＣ）と称するＧＳＭネットワークの特殊目的の要素に記憶される。ＡＵＣは、Ａ８と称する暗号化アルゴリズムと、Ａ３と称する確証アルゴリズムと、ランダム番号ＲＡＮＤの発生機能も備えている。暗号キーＫｃと称するパラメータがアルゴリズムＡ８によりＫｉ及びＲＡＮＤから発生される。同様に、符号応答ＳＲＥＳと称するパラメータが、アルゴリズムＡ３によりＫｉ及びＲＡＮＤから発生される。３つのパラメータＲＡＮＤ、Ｋｃ及びＳＲＥＳは、更なる確証及び暗号化に使用されるべき加入者特有の「トリプレット（３つ組）」を形成する。必要になるたびにトリプレットが計算されて転送されるのを回避するために、ＡＵＣ／ＨＬＲにより各加入者ごとに前もって多数のトリプレットが計算され、そして要求時応じて、ビジター位置レジスタ（ＶＬＲ）及び移動サービス交換センター（ＭＳＣ）へ送られて、そこに記憶される。ＭＳＣ／ＶＬＲは、そのビジター加入者の各々に対して少なくとも１つの未使用のトリプレットを常に有する。厳密なセキュリティは、１つの通信に対してトリプレットが１回だけ使用され、そして破壊されることを要求する。加入者がその全ての使用可能なトリプレットを使用すると、ＡＵＣ／ＨＬＲは、新たな一連のトリプレットを計算して返送することが要求される。

ＧＳＭ移動ステーションは、２つの部分に分割され、その一方の部分は、無線インターフェイス及び移動装置に特有のハードウェア及びソフトウェアを含み、そして別の部分は、加入者特有のデータ、即ち加入者認識モジュール即ちＳＩＭを含む。各加入者は、通常は、スマートカードの形態でＳＩＭを有し、これは、移動ステーション側のほとんどのセキュリティ機能に対し責任を負う。これは、Ｋｉ、確証アルゴリズムＡ３、暗号化アルゴリズムＡ８、及びネットワーク側から受け取った暗号化キーＫｃを記憶する。

確証の間に、ＶＬＲ／ＭＳＣは、トリプレットのランダム番号ＲＡＮＤ（及びＫｃも）を移動ステーションに送信する。移動ステーション、特に、ＳＩＭは、確証アルゴリズムＡ３及び確証キーＫｉを用いてＲＡＮＤを処理し、そしてそれにより得られる符号応答ＳＲＥＳをＶＬＲ／ＭＳＣに返送する。このＳＲＥＳはＨＬＲにより与えられたトリプレットのＳＲＥＳに対してチェックされる。２つ

のＳＲＥＳが互いに等しい場合には、アクセスが許され、さもなくば、拒絶される。

ＧＳＭの全てのセキュリティ機構は、確証キーＫｉの機密性に依存する。Ｋｉは決して送信されず且つＡＵＣ／ＨＬＲから決して出ない。又、ＳＩＭは、Ｋｉを読み取りに対して完全に保護する。数学的アルゴリズムＡ３は、一方向にしか働かない（一方向トラップドア機能）ので、送信されたＲＡＮＤ－ＳＲＥＳ対からキーＫｉを導出することは不可能である。更に、確証アルゴリズムＡ３自体は機密のアルゴリズムであり、ＧＳＭ仕様において見つけることができない。この仕様は、ＲＡＮＤ及びＳＲＥＳを知った上でのＫｉの計算をできるだけ複雑にしなければならないことを要求するだけである。このレベルの複雑さは、どのセキュリティレベルが達成されたかを決定する。この要求を越えてＡ３に課せられる唯一の制約は、入力パラメータのサイズ（ＲＡＮＤは長さが１２８ビット）及び出力パラメータのサイズ（ＳＲＥＳは長さが３２ビットなければならない）である。Ｋｉは、ＡＵＣ／ＨＬＲに記憶されるときはいかなるフォーマット及び長さでもよいが、Ｋｉがネットワークにおいて搬送される場合だけは、１２８ビットの最大長さに制約される。実際に、移動ステーション及びインフラストラクチャーの両方におけるＧＳＭの設計選択は、オペレータが、他のオペレータとは独立してそれ自身の加入者に適用できるＡ３を選択できるようにする。

米国内では、パーソナルコミュニケーションシステム（ＰＣＳ）と称するデジタルセルラーシステムが開発中である。このＵＳ　ＰＣＳは、特に、セキュリティ機能を含むネットワークアーキテクチャー及びプロトコルに関してＧＳＭシステムに著しく依存している。しかしながら、システムの種々の部分において幾つかの僅かな変更がなされる。１つの潜在的な変更は、ＧＳＭシステムに使用される確証アルゴリズムＡ３がＵＳ　ＰＣＳのＣＡＶＥアルゴリズムに置き換えられることである。というのは、ＣＡＶＥアルゴリズムは、米国内で開発されたものであり、アナログＡＭＰＳ（アドバンスト・モービル・ホーン・サービス）ネットワークに既に使用されているからである。ＰＣＳシステムにおいて確証のために使用するのに適したＣＡＶＥアルゴリズムは、多数の連結情報フィールドより成る１５２ビットの入力パラメータと、１８ビットの出力パラメータとを有し、

これに対して、ＧＳＭのＡ３アルゴリズムは、１２８ビットのＫｉ及びＲＡＮＤパラメータを入力パラメータとして有しそして３２ビットのＳＲＥＳパラメータを出力パラメータとして有する。それ故、ＧＳＭベースの移動通信システムにおいてＡ３をＣＡＶＥアルゴリズムに置き換えることは、更なる変更なしに行うことができない。しかしながら、これらの変更は、システム全体にわたって種々のプロトコル、機能、メッセージ及びデータ構造に明らかに影響を及ぼし、ＣＡＶＥアルゴリズムが技術的にも経済的にも魅力的ではなくなる。更に別の欠点は、ＧＳＭシステムとの互換性が失われ、従って、例えば、ＳＩＭがＧＳＭシステムとＵＳ　ＰＣＳシステムとの間をローミングすることができなくなる。

発明の要旨

本発明の目的は、ＧＳＭシステム又はＧＳＭをベースとする移動通信ネットワークにおいてＧＳＭの確証パラメータの変更を招くことなくＣＡＶＥアルゴリズムをＡ３アルゴリズムとして使用できるようにすることである。

本発明の別の目的は、ＧＳＭシステム又はＧＳＭをベースとする移動通信ネットワークにおいてＧＳＭのトリプレットデータ構造を変更することなくＣＡＶＥアルゴリズムをＡ３アルゴリズムとして使用できるようにすることである。

本発明の更に別の目的は、ＧＳＭシステム又はＧＳＭをベースとする移動通信ネットワークにおいて標準的なＧＳＭシステムのセキュリティ機能を保持しながらＣＡＶＥアルゴリズムをＡ３アルゴリズムとして使用できるようにすることである。

本発明の１つの特徴は、第１の確証応答計算方法と共に使用されるよう意図された確証手順を使用し；上記第１の確証応答計算方法に代わって第２の確証応答計算方法を使用し；上記第１の確証応答計算方法には適合するが上記第２の確証応答計算方法には適合しない確証キーを上記移動通信ネットワークの各加入者ごとに与え；上記第１の確証応答計算方法には適合するが上記第２の確証応答計算方法には適合しないランダム番号を発生し；上記確証キー及び上記ランダム番号から上記第２の確証応答計算方法に適合する入力パラメータを導出し；上記移動通信ネットワークに使用される上記確証手順の確証応答フォーマットに適合しない確証応答を上記第２の確証応答計算方法により計算し；この確証応答を上記確

証手順の確証応答フォーマットに適合するフォーマットに変更し；そして上記確証応答を上記確証手順に適合する上記フォーマットで移動通信ネットワークにおいて転送して記憶する、という段階を備えた移動通信ネットワークのための確証方法に係る。

本発明によれば、ＣＡＶＥアルゴリズムの入力パラメータと、ＧＳＭ型の入力パラメータ、即ちランダム番号ＲＡＮＤ及び確証キーＫｉとの間、及びＣＡＶＥアルゴリズムの出力パラメータと、ＧＳＭの出力パラメータ、即ち符号応答ＳＲＥＳとの間に、パラメータ適応機能が与えられる。その結果、ＣＡＶＥアルゴリズム自体に変更は必要とされず、又、確証センターのＡＵＣ／ＨＬＲ及び移動ステーションＭＳにおいてＳＲＥＳを計算する以外、ＧＳＭ型のセキュリティ機能から何ら逸脱する必要もない。

図面の簡単な説明

以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。

図１は、ＧＳＭをベースとするセルラー移動無線システムを示すブロック図である。

図２は、確証センターＡＵＣにおける公知の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図３は、移動ステーションＭＳにおける公知の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図４は、ＭＳＣ／ＶＬＲにおける確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図５は、確証及び暗号化パラメータの発生、転送及び使用に関連した信号を示す図である。

図６は、確証センターＡＵＣにおける本発明の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

図７は、移動ステーションＭＳにおける本発明の確証及び暗号化パラメータ処理ユニットの機能的ブロック図である。

好ましい実施形態の詳細な説明

本発明は、パン・ヨーロピアンデジタル移動無線システムＧＳＭ又はＧＳＭをベースとする移動無線システム、例えば、ＤＣＳ１８００デジタル通信システム及び米国のパーソナル・コミュニケーション・システム（ＰＣＳ）と称するデジタルセルラーシステムに適用することができる。本発明の好ましい実施形態は、標準のＧＳＭシステムに適用するものとして以下に説明するが、その主たる適用分野は、米国のＰＣＳシステムであることが明らかである。ＧＳＭシステムの構造及び動作は、当業者に良く知られており、ヨーロピアン・テレコミュニケーションズ・スタンダーズ・インスティテュートＥＴＳＩで発行されたＧＳＭ仕様書に定義されている。移動通信のためのＧＳＭシステム、Ｍ．モーリ及びＭ．ポーテット、パライゼウ、フランス、１９９２年；ＩＳＢＮ２－９５０７１９０－０－７も参照されたい。

ＧＳＭシステムの基本的構造が図１に示されている。

ＧＳＭ構造体は、２つの部分、即ちベースステーションシステム（ＢＳＳ）とネットワークサブシステム（ＮＳＳ）とで構成される。ＢＳＳ及び移動ステーションＭＳは、無線接続を経て通信する。ＢＳＳにおいて、各セルは、ベーストランシーバステーション（ＢＴＳ）によりサービスされる。ＢＴＳのグループは、ベースステーションコントローラ（ＢＳＣ）に接続され、その機能は、ＢＴＳにより使用される無線周波数及びチャンネルを管理することである。ＢＳＣは、移動サービス交換センター（ＭＳＣ）に接続される。ＭＳＣは、少なくとも１つの移動ステーションＭＳを含むコールを交換するためのものである。幾つかのＭＳＣが、公衆交換電話ネットワーク（ＰＳＴＮ）のような他のテレコミュニケーションネットワークに接続され、これらネットワークとコールをやり取りするためのゲートウェイ機能を含む。これらＭＳＣは、ゲートウェイＭＳＣ（ＧＭＳＣ）として知られている。

コールのルート指定に関連したデータベースには、２つの主たる形式がある。ホーム位置レジスタ（ＨＬＲ）は、ネットワークの全ての加入者に関する加入者データを永久的又は半永久的に記憶し、このデータは、加入者がアクセスできるサービスや、加入者の現在位置に関する情報を含む。第２の形式のレジスタは、

ビジター位置レジスタ（ＶＬＲ）である。ＶＬＲは、一般には、１つのＭＳＣに取り付けられるが、多数のＭＳＣにサービスすることもできる。この統合されるネットワーク要素は、ビジターＭＳＣ（ＶＭＳＣ）として知られている。移動ステーションＭＳがアクティブ（登録されて、コールを発したり受けたりできる）であるときには、ＨＬＲに保持された移動ステーションＭＳに関する移動加入者データのほとんどが、移動ＭＳが存在するエリアのＭＳＣのＶＬＲへダウンロード（コピー）される。

上記したように、移動無線サービスにおいては、第三者による不許可のコールの試みや、侵入又は傍聴を防止するように多大な注意を払わねばならない。ＧＳＭシステムの保護機構は、発呼又は被呼移動ステーションの確証を得、そして暗号化キーを用いて、トラフィックチャンネルのスピーチ及びデータをエンコードする。

確証及び暗号化キーを与えるためのＧＳＭ仕様に基づく公知の機能を、図２、３、４及び５を参照して以下に説明する。

加入時に、加入者確証キー（Ｋｉ）と称する機密番号が、国際移動加入者認識（ＩＭＳＩ）と共に移動加入者に割り当てられる。図２に示すように、確証センターＡＵＣは、ＧＳＭネットワークの各移動加入者に対する確証キーＫｉを記憶するデータベース２０を備えている。移動加入者のＫｉは、移動加入者のＩＭＳＩをインデックスとして使用してデータベース２０から検索することができる。ＡＵＣには、更に、暗号化アルゴリズムＡ８、確証アルゴリズムＡ３及びランダム番号ジェネレータ２１が設けられている。ランダム番号ジェネレータ２１は、長さが１２８バイトのランダム番号ＲＡＮＤを与える。データベース２０から検索されたキーＫｉ及びランダム番号ジェネレータ２１からのランダム番号ＲＡＮＤは、確証アルゴリズムＡ３において入力パラメータとして使用され、符号応答ＳＲＥＳを計算すると共に、暗号化アルゴリズムＡ８において入力パラメータとして使用されて、トラフィックチャンネルエンコードのための暗号化キーＫｃを計算する。３つのパラメータＲＡＮＤ、ＳＲＥＳ及びＫｃは、移動加入者のためのトリプレット（３つ組）を形成する。

トリプレットは、更に、以下に詳細に述べるように、確証及び暗号化に使用す

るために訪問先のＭＳＣ／ＶＬＲへ転送される。

トリプレットは、１つの通信に対して１回だけ使用されて、破壊される。必要とされるたびにトリプレットを計算して転送するのを回避するために、ＡＵＣ／ＨＬＲにより各移動加入者ごとに多数のトリプレットが前もって計算され、そして要求に応じて訪問先のＭＳＣ／ＶＬＲへ供給され、そこに記憶される。

訪問先のＭＳＣ／ＶＬＲは、加入者ごとに幾つかのこのようなトリプレットの保存情報を、必要に応じて検索するために記憶する。図４には、訪問先のＭＳＣ／ＶＬＲに維持されたセキュリティパラメータファイル４０が例示されている。このファイル４０は、各ＩＭＳＩ（加入者）ごとにｎ個のトリプレット１・・・ｎを含む。

セキュリティパラメータファイル４０のこの保存情報は、移動加入者が最初に訪問先のＭＳＣ／ＶＬＲに登録されるときに最初に確立され、即ちこれは、ＨＬＲから「加入者データ挿入」メッセージにおいてダウンロードされる加入者データの一部分である。加入者が、使用可能な全てのトリプレットを使用してしまうと、ＡＵＣ／ＨＬＲは、新たな一連のトリプレットを計算して返送するよう要求される。図５を参照すれば、このトリプレット補充手順は、「パラメータ送信」メッセージと、その返答である「パラメータ送信結果」メッセージの２つのメッセージで構成される。前者のメッセージは、図２について述べたように、トリプレットを計算するためにＫｉを検索するのに使用される移動加入者のＩＭＳＩを含む。計算されたトリプレットは、「パラメータ送信結果」メッセージＭＳＣ／ＶＬＲへ送られ、そしてＶＬＲに記憶される。

更に、図４を参照すれば、移動ステーションＭＳは、アクセス要求をＭＳＣ／ＶＬＲへ送信する。ＭＳＣ／ＶＬＲは、ＩＭＳＩをインデックスとして使用してセキュリティパラメータファイルに移動ステーションＭＳの加入者に対して保存されたトリプレットの１つを検索する。ＭＳＣ／ＶＬＲは、一方では、トラフィックチャンネルの暗号化に使用されるべきＫｃの値をＢＳＣのチャンネル装置へ搬送し、そして他方では、図４にブロック４１で示したように、ＲＡＮＤの値を「確証要求」メッセージにおいてＭＳへ搬送する。移動ステーションＭＳは、ＲＡＮＤに基づいて、トリプレットの他の値（ＳＲＥＳ及びＫｃ）を計算する。

図３を参照すれば、ＭＳは、移動加入者の暗号キーＫｉのコピーと、暗号化アルゴリズムＡ８と、確証アルゴリズムＡ３とを記憶する。ＭＳＣ／ＶＬＲのための「確証要求」メッセージを受け取ると、ＭＳは、このメッセージからＲＡＮＤを抽出し、そしてこのＲＡＮＤ及び記憶されたＫｉをアルゴリズムＡ３及びＡ８に入力し、各々符号応答ＳＲＥＳ及び暗号キーＫｃを各々計算する。計算されたＳＲＥＳは、「確証結果」メッセージにおいてＭＳＣ／ＶＬＲへ搬送され、図４及び５に示すように確証が完了する。

図４を参照すれば、ＭＳＣ／ＶＬＲは、「確証結果」メッセージからＳＲＥＳの値を抽出し（ブロック４２）、そしてファイル４０からＳＲＥＳの記憶された値を検索する（ブロック４３）。次いで、この通信のために、他の処理の前に、ＭＳＣ／ＶＬＲは、ＡＵＣ／ＨＬＲで計算されたＳＲＥＳが、ＭＳで計算されたＳＲＥＳと同じであることをチェックすることにより（ブロック４４）移動加入者を「確証」する。２つの値が同一の場合には、アクセスが許可される（ブロック４５）。２つの値が同一でない場合には、アクセスが拒絶される（ブロック４６）。

暗号化手順は、本発明には関与せず、ここでは詳細に説明しない。

本発明の先行技術で述べたように、特にセキュリティ機能を含むネットワークアーキテクチャー及びプロトコルに関してＧＳＭシステムに大きく依存するパーソナルコミュニケーションシステム（ＰＣＳ）と称する米国内のデジタルセルラーシステム又は他のセルラーシステムにおいてはＣＡＶＥアルゴリズムを確証アルゴリズムＡ３として使用する必要がある。ＣＡＶＥアルゴリズムは、米国内で開発され、ＣＡＶＥアルゴリズム情報の入手性は、ＩＴＡＲ（米国のインターナショナル・トラフィック・アンド・アームズ・レギュレーション）の管理下にある。しかしながら、ＣＡＶＥは、アナログＡＭＰＳ（アドバンスト・モービル・ホーン・サービス）ネットワークに既に使用されており、その入力／出力パラメータは、ＥＩＡ／ＴＩＡ規格ＩＳ－５４に規定されている。ＣＡＶＥアルゴリズムは、多数の連結情報フィールドより成る１５２ビットの入力パラメータと、１８ビットの出力パラメータとを有する。しかしながら、実際に実施する場合にはＧＳＭシステムのＡ３アルゴリズムが１２８ビットのＫｉ及びＲＡＮＤを入力

パラメータとして有しそして３２ビットのＳＲＥＳを出力パラメータとして有するために問題に遭遇する。

これらの問題は、本発明により、ＣＡＶＥアルゴリズムの入力及び出力においてパラメータの適応を行ったときに克服される。その結果、ＣＡＶＥアルゴリズム自体に何の変更も必要とされず、又、ＡＵＣ／ＨＬＲ及びＭＳにおいてＳＲＥＳを計算すること以外、ＧＳＭ仕様から何ら逸脱する必要もない。

本発明によるパラメータ適応の好ましい実施形態を図６及び７について以下に説明する。

図６を参照すれば、本発明による確証センターＡＵＣは、図２に示されたデータベース２０及びジェネレータ２１と同様のデータベース６０及びランダム番号ジェネレータ６１を備えている。データベース６０は、ＩＭＳＩでインデックスされるＧＳＭネットワークの全ての移動加入者に対しＧＳＭ仕様に基づいて１２８ビットの確証キーＫｉを記憶する。更なる計算のためにＫｉを選択するところのＩＭＳＩは、信号インターフェイス６７から受け取られ、この信号インターフェイスは、ＨＬＲ又はＶＬＲから、例えば、「パラメータ送信」メッセージにおいてそれを受け取る。ランダム番号ジェネレータ６１は、１２８ビットのランダム番号ＲＡＮＤをＧＳＭ仕様に基づいて発生する。

Ｋｉ及びＲＡＮＤは、暗号化アルゴリズムＡ８に入力され、このアルゴリズムは、ＧＳＭの仕様に基づいて６４ビットの暗号化キーＫｃを計算する。換言すれば、Ｋｃの計算は、図２を参照して説明したものと同じである。

又、１２８ビットのＲＡＮＤは、裁断ユニット６２にも入力され、該ユニットは、ＲＡＮＤを２４ビットの裁断されたＲＡＮＤ（ＴＲＡＮＤ）へと裁断する。ＴＲＡＮＤは、例えば、ＲＡＮＤの最上位２４ビットを含む。しかしながら、ここで使用する裁断動作は、１２８ビットのランダム番号ＲＡＮＤから２４ビットのランダム番号ＴＲＡＮＤを導出するためのいかなる方法も包含することが明らかである。Ｋｉの長さは、好ましい実施形態では１２８ビットであるが、１２８以下の整数をＮとすれば、Ｎビットの長さでよいことに注意されたい。従って、ＴＲＡＮＤの長さＭは、Ｎに依存し、Ｍ＝１５２－Ｎビットである。

２４ビットのＴＲＡＮＤは、次いで、合成ユニット６３に入力され、該ユニッ

ト６３の他方の入力は、１２８ビットの確証キーＫｉである。合成ユニット６３の出力は、Ｋｉ及びＴＲＡＮＤの１５２ビットの組合せＣＯＭＰである。ＣＯＭＰの最上位１２８ビットは、Ｋｉを含み、そして最下位２４ビットは、ＴＲＡＮＤを含む。しかしながら、ここで使用する合成動作は、ＫｉとＴＲＡＮＤを合成することにより１５２ビット値を導出するための例えば論理演算のような方法を包含することが明らかである。

１５２ビットのＣＯＭＰパラメータは、計算ユニット６５においてＣＡＶＥアルゴリズムの入力パラメータに設定される要件を満足する。従って、本発明によるパラメータ適応は、ＧＳＭ適合の入力パラメータＫｉ及びＲＡＮＤからＣＡＶＥ適合の入力パラメータを導出する。計算の結果として、ＣＡＶＥ計算ユニット６５は、１８ビットの出力パラメータを出力する。

ＣＡＶＥからの１８ビットの出力パラメータは、次いで、パッドユニット６４に入力され、ここでは、１４のスタフビットが挿入されて、３２ビット値が得られる。１４のスタフビットは、例えば、３２ビットパラメータの最下位１４ビットを確立し、最上位１８ビットは、ＣＡＶＥ６５からの１８ビット出力を含む。しかしながら、ここで使用するパッド動作は、１８ビットのＣＡＶＥ出力パラメータを１４ビットだけ延長して３２ビットを得るための例えば論理演算のような何らかの方法を包含することが明らかであろう。

これにより得られる３２ビットの出力パラメータは、次いで、ＧＳＭ仕様に基づく符号応答ＳＲＥＳとして使用される。従って、本発明によるパラメータ適応は、ＣＡＶＥ適合出力パラメータからＧＳＭ適合の出力パラメータを導出する。

３つのＧＳＭ適合のセキュリティパラメータＳＲＥＳ、Ｋｃ及びＲＡＮＤは、標準的なＧＳＭトリプレットを形成するトリプレット形成ユニット６６に入力される。トリプレットは、信号インターフェイス６７を経てＨＬＲ又はＶＬＲに転送される。従って、ＳＲＥＳは、標準的なＳＲＥＳと同様に、ＧＳＭネットワークにおいて転送されそして処理される。

図７を参照すれば、本発明による移動ステーションＭＳは、移動加入者の暗号キーＫｉのコピーをメモリ７５に記憶する。又、ＭＳは、暗号化アルゴリズムＡ８を実行する計算ユニット７６と、確証のためのＣＡＶＥアルゴリズムを実行

する計算ユニット７７とを備えている。ＭＳＣ／ＶＬＲから「確証要求」メッセージを受け取ると、無線インターフェイスに特有のハードウェア及びソフトウェアを含むＭＳの移動装置７８は、メッセージからＲＡＮＤを抽出し、そしてＲＡＮＤ及び記憶されたＫｉをＡ８計算ユニット７６へ入力し、暗号キーＫｃを計算する。本発明の好ましい実施形態では、７８を除く全ての機能ブロックが、ＭＳの加入者認識モジュール即ちＳＩＭに配置されている。

又、１２８ビットのＲＡＮＤは、ＲＡＮＤを２４ビットのＴＲＡＮＤに裁断する裁断ユニット７２にも入力される。裁断ユニット７２は、図６に示す裁断ユニット６２と同一である。

２４ビットのＴＲＡＮＤは、次いで、１２８ビットのＫｉと共に、合成ユニット７３に入力される。合成ユニット７３の出力は、１５２ビットのＣＯＭＰである。合成ユニット７３は、図６に示す合成ユニット６３と同一である。

１５２ビットのＣＯＭＰは、次いで、ＣＡＶＥ計算ユニット７７に入力され、該ユニットは、１８ビットの出力パラメータを出力する。

ＣＡＶＥ７７からの１８ビット出力パラメータは、パッドユニット７４に入力され、ここで、１４のスタフビットが取り付けられて、３２ビット値が与えられる。パッドユニット７４は、図６に示すパッドユニット６４と同一である。

それにより得られた３２ビットの出力パラメータは、次いで、ＧＳＭ仕様に基づくＳＲＥＳパラメータとして使用される。ＳＲＥＳは、移動装置７８に返送され、そして更に「確証結果」メッセージにおいてＭＳＣ／ＶＬＲへ送られ、標準的なＧＳＭシステムの場合と同様にＭＳＣ／ＶＬＲにおいて処理される。

ＮビットのＫｉ及びＲＡＮＤパラメータから１５２ビットのＣＡＶＥ入力パラメータを導出する別の実施形態が図８に示されている。以下の例では、Ｎ＝１２８であるが、これらの実施形態ではいかなる正の整数でもよい。Ｋｉは、２つの部分に分割され、即ちＫｉの１０４ビット、例えば、１０４のＬＳＢビットは、論理ユニット８１の入力に送られる。Ｋｉの残りの２４ビットは、合成器８２に入力される。同様に、ＲＡＮＤも２つの部分に分割され、即ちＲＡＮＤの１０４ビット、例えば、１０４のＭＳＢビットは、論理ユニット８１に入力される。ＲＡＮＤの残りの２４ビットは、合成器８２の別の入力に送られる。２つの

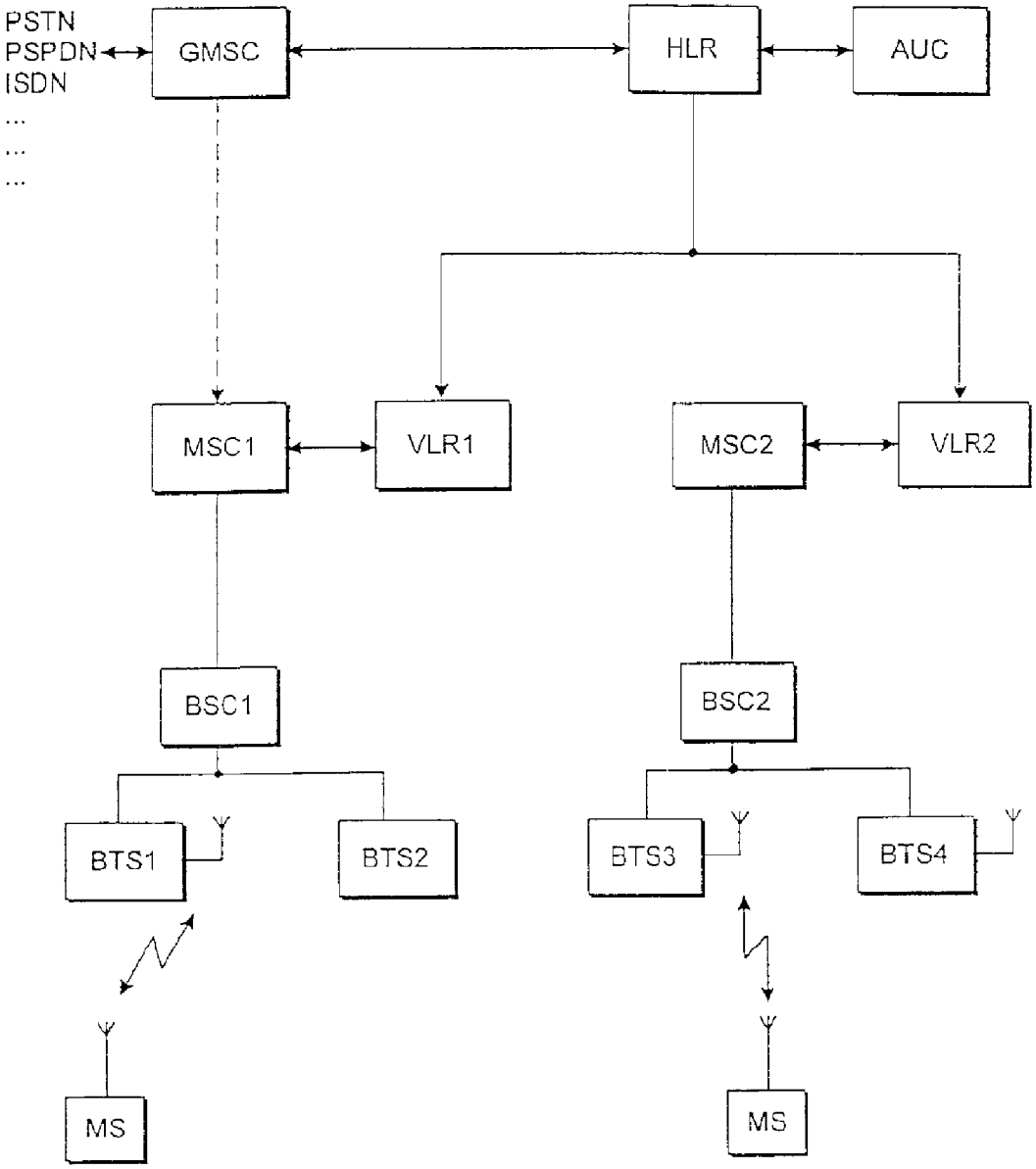
１０４ビット入力の間でアンド、オア又は排他的オア（ＸＯＲ）のような論理演算が行われ、単一の１０４ビット出力が与えられる。論理ユニット８１からの１０４ビット出力は、合成器８２に入力される。合成器８２は、２つの２４ビット入力と１０４ビット入力を１５２ビットパラメータへと組み立て、ＣＡＶＥアルゴリズムへ入力する。図６の確証センター及び図７の移動ステーションに適用されるときは、論理ユニット８１及び合成器８２が、各々、裁断ユニット６２、７２及び合成器６３、７３に置き換えられる。

図８の実施形態に対する更に別の変更として、Ｋｉの１０４ビット及びＲＡＮＤの１０４ビットが同数のサブブロックに細分化され、異なるサブブロック間で異なる論理演算が実行される。例えば、２６ビットの４つのサブブロックが存在する。

添付図面及びそれを参照した以上の説明は、単に本発明を例示するものに過ぎない。請求の範囲から逸脱せずに多数の変更や修正がなされ得ることが当業者に明らかであろう。

【図１】

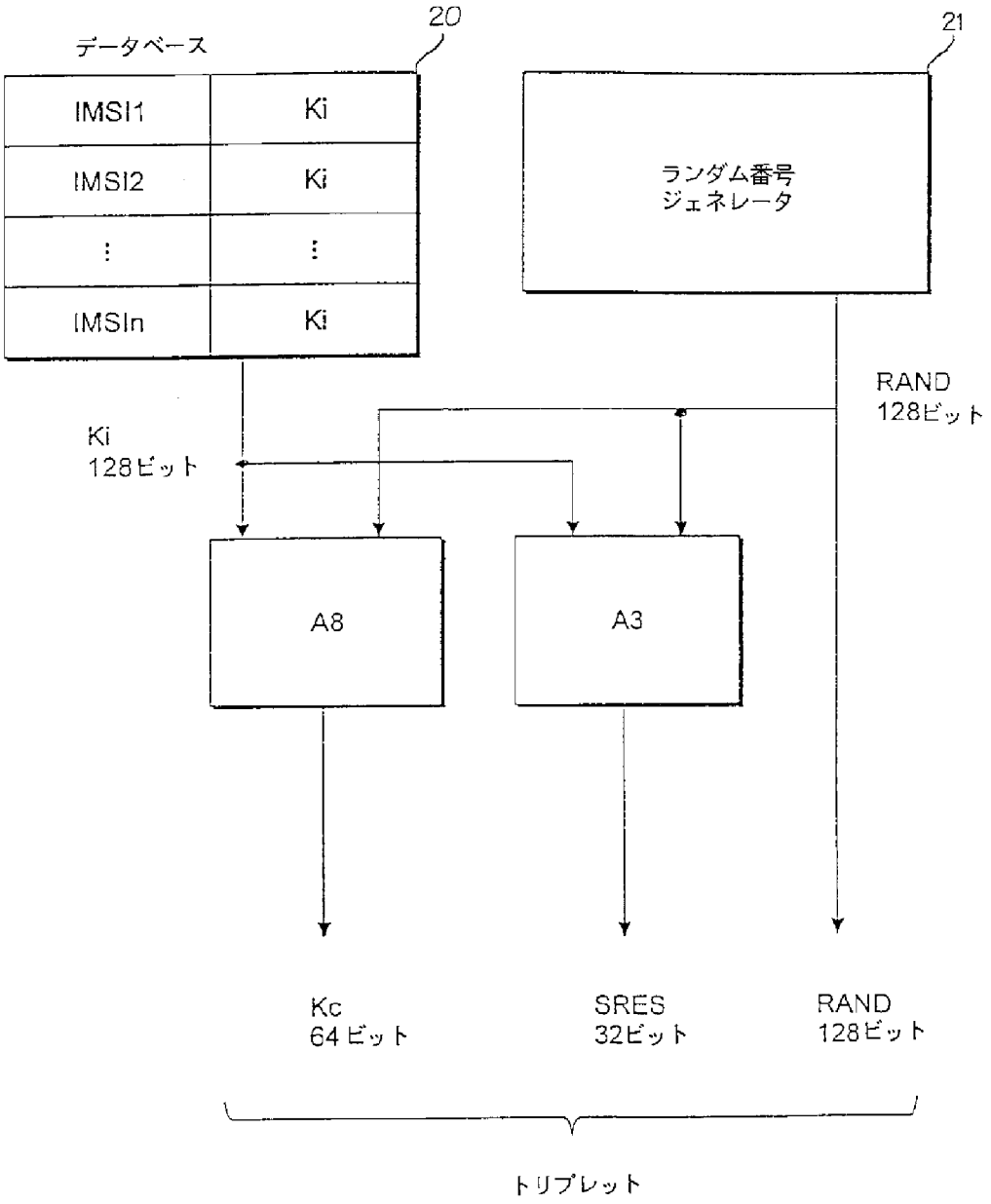
Fig. 1
（　従来例　）


PSTN
PSPDN
ISDN
...
...
...
GMSC
HLR
AUC
MSC1
VLR1
MSC2
VLR2
BSC1
BSC2
BTS1
BTS2
BTS3
BTS4
MS
MS

【図２】

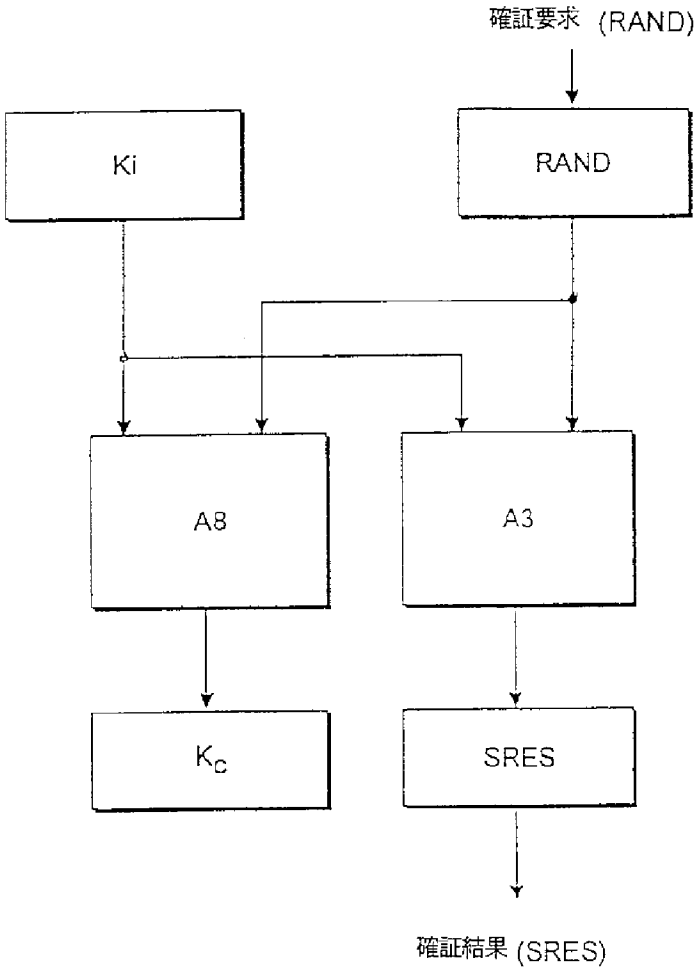
Fig. 2

（ 従来例 ）


20
データベース
IMSI1
Ki
IMSI2
Ki
IMSIn
Ki
21
ランダム番号
ジェネレータ
RAND
128ビット
Ki
128ビット
A8
A3
Kc
64ビット
SRES
32ビット
RAND
128ビット
トリプレット

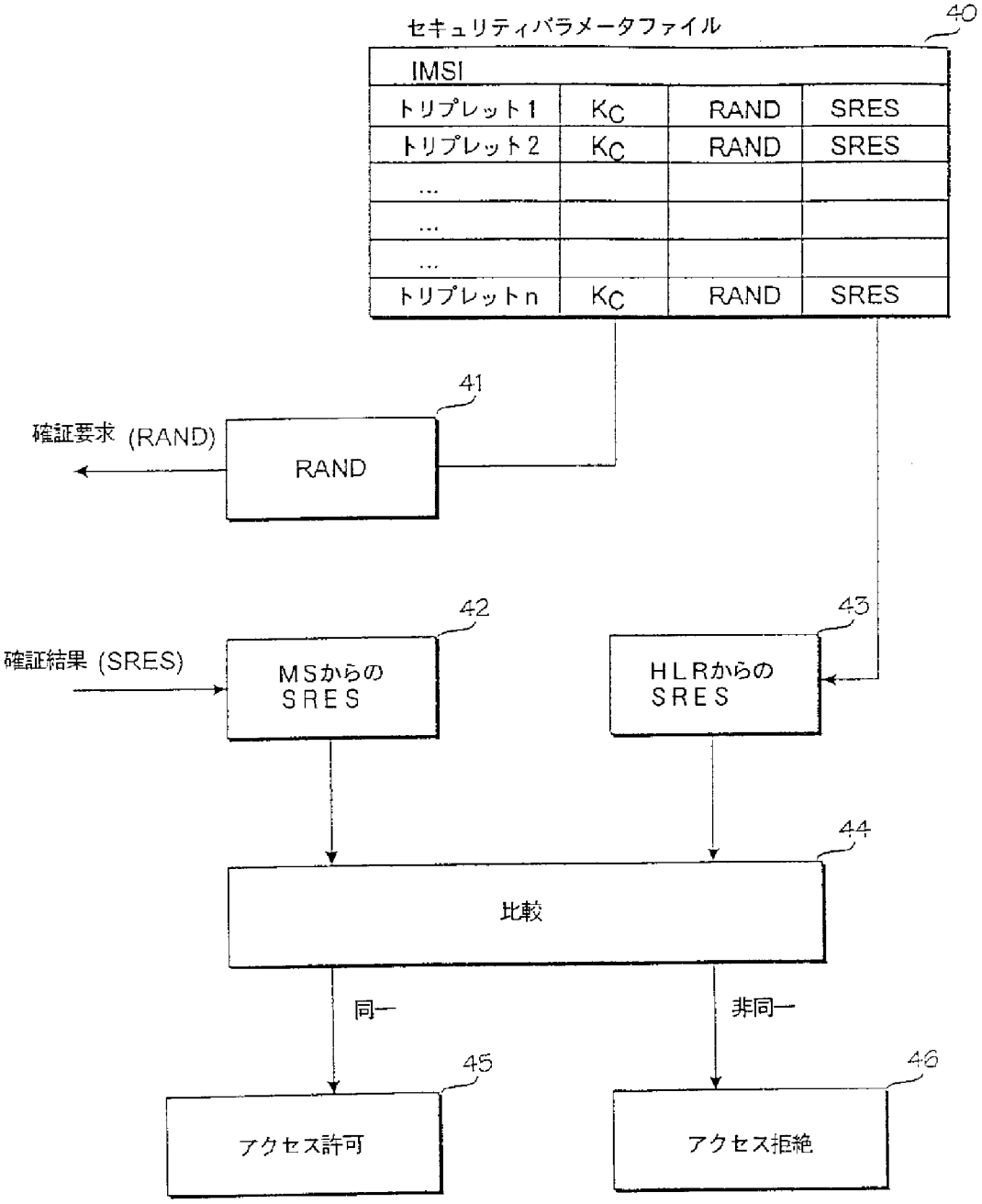
【図３】

Fig. 3
（　従来例　）



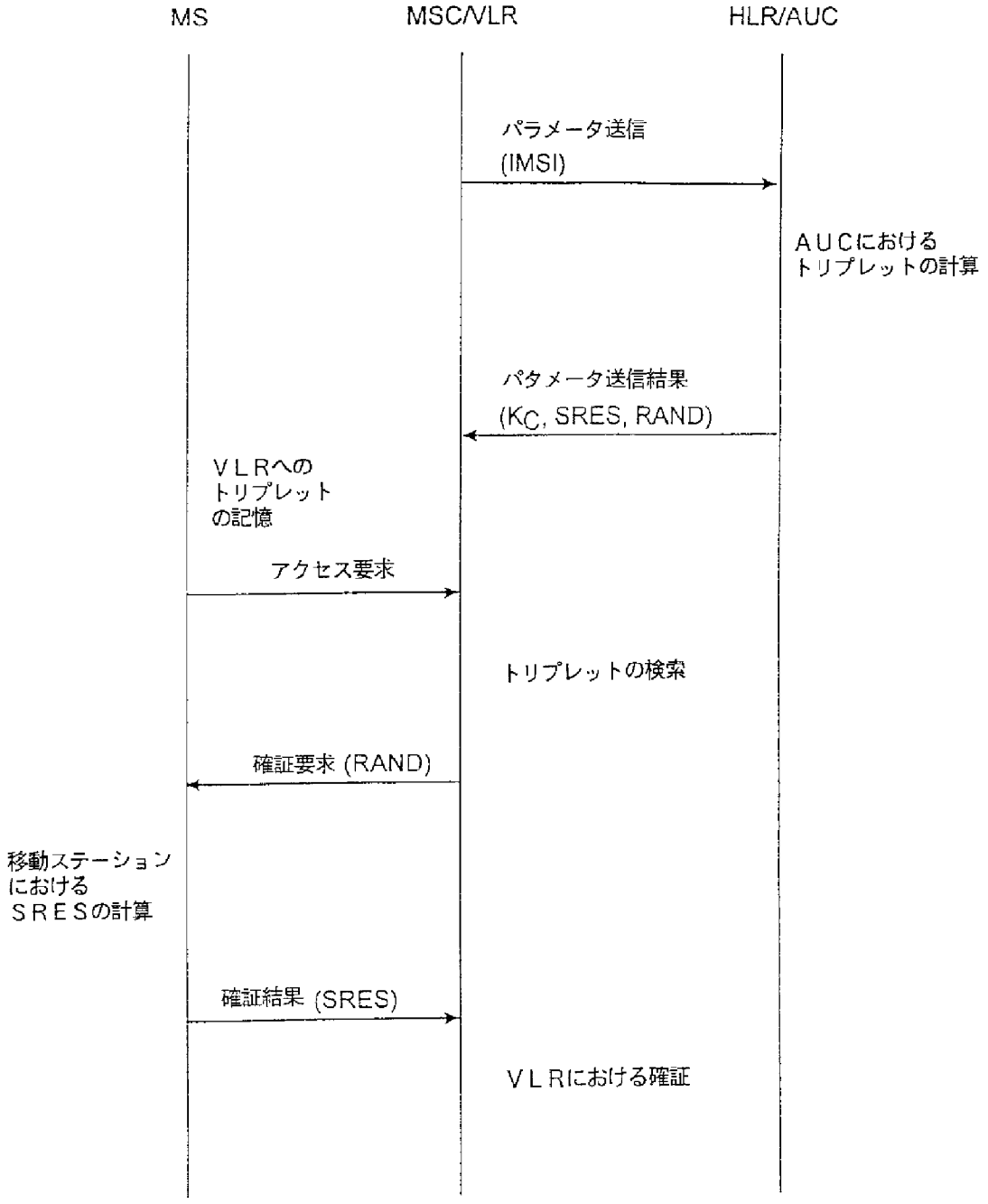
【図４】

Fig. 4
（　　従来例　）


セキュリティパラメータファイル
40
IMSI
トリプレット1
Kc
RAND
SRES
トリプレット2
Kc
RAND
SRES
...
...
...
トリプレットn
Kc
RAND
SRES
41
確証要求 (RAND)
RAND
42
確証結果 (SRES)
MSからの SRES
43
HLRからの SRES
44
比較
同一
非同一
45
アクセス許可
46
アクセス拒絶

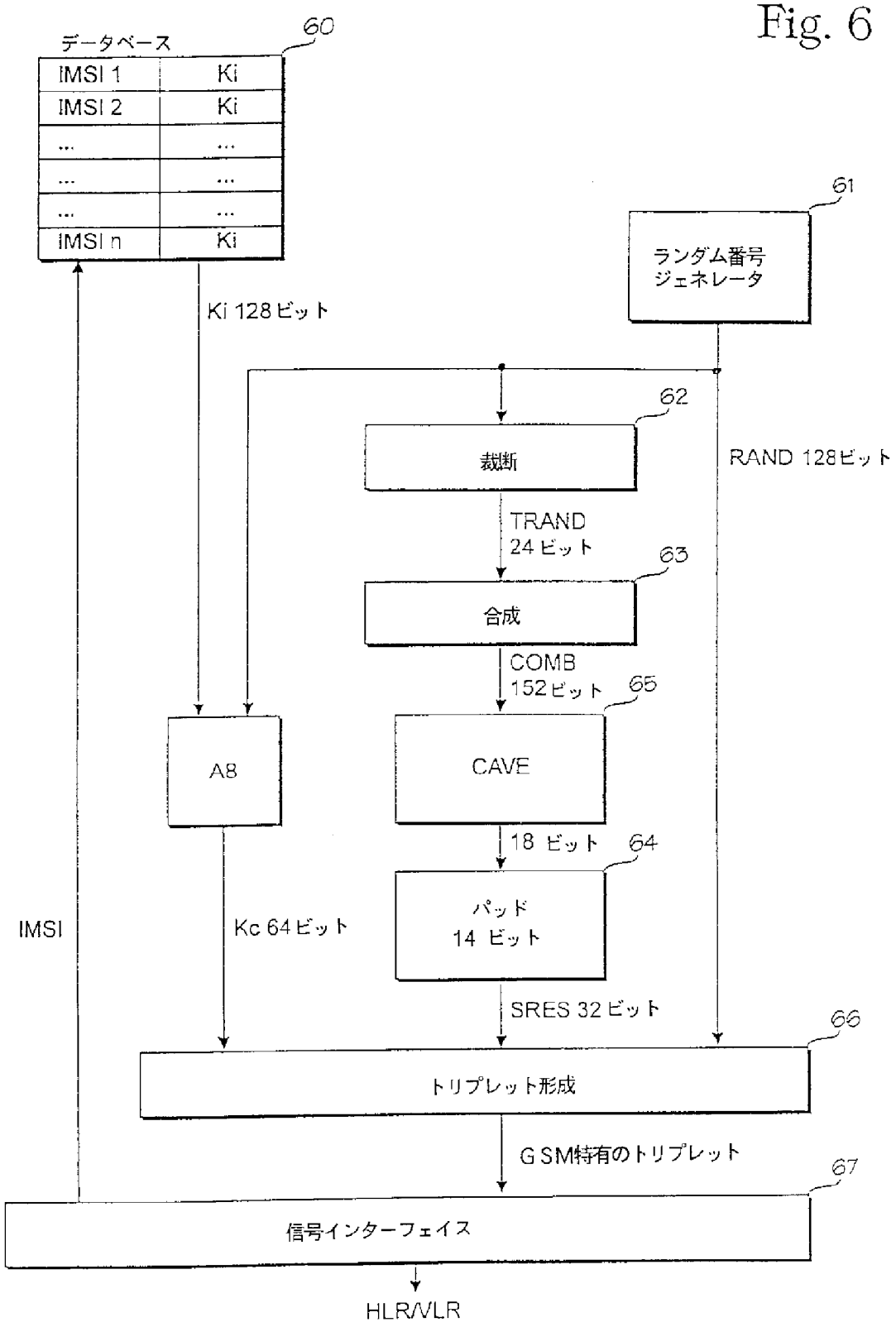
【図５】

Fig. 5
（　従来例　）


MS
MSC/VLR
HLR/AUC
パラメータ送信
(IMSI)
ＡＵＣにおける
トリプレットの計算
パタメータ送信結果
(KC, SRES, RAND)
ＶＬＲへの
トリプレット
の記憶
アクセス要求
トリプレットの検索
確証要求 (RAND)
移動ステーション
における
ＳＲＥＳの計算
確証結果 (SRES)
ＶＬＲにおける確証

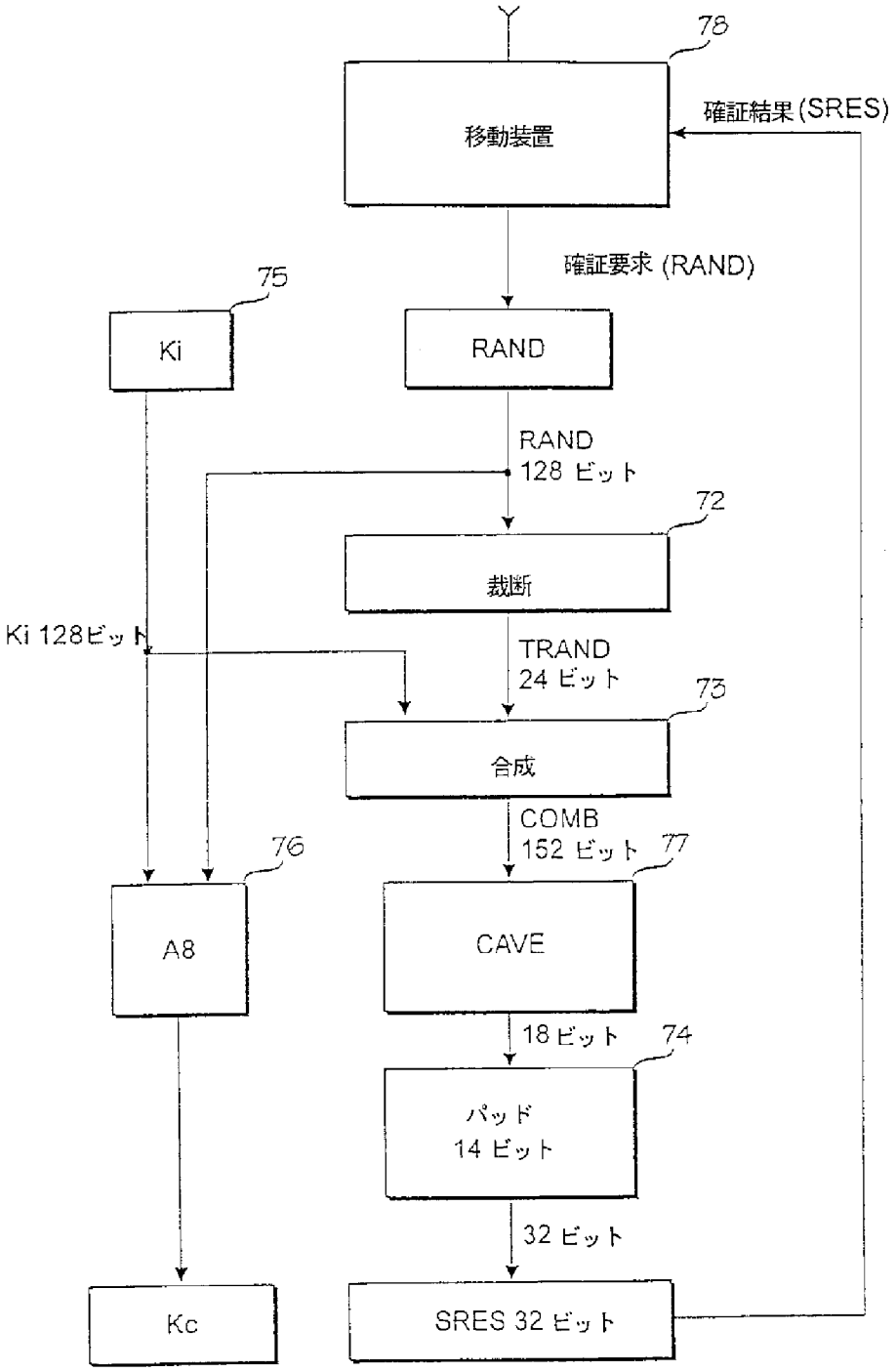
【図６】

Fig. 6


データベース
60
IMSI 1
Ki
IMSI 2
Ki
...
...
...
...
...
...
IMSI n
Ki
Ki 128ビット
61
ランダム番号
ジェネレータ
62
裁断
RAND 128ビット
TRAND
24ビット
63
合成
COMB
152ビット
65
CAVE
A8
18 ビット
64
パッド
14 ビット
IMSI
Kc 64ビット
SRES 32ビット
66
トリプレット形成
GSM特有のトリプレット
67
信号インターフェイス
HLR/VLR

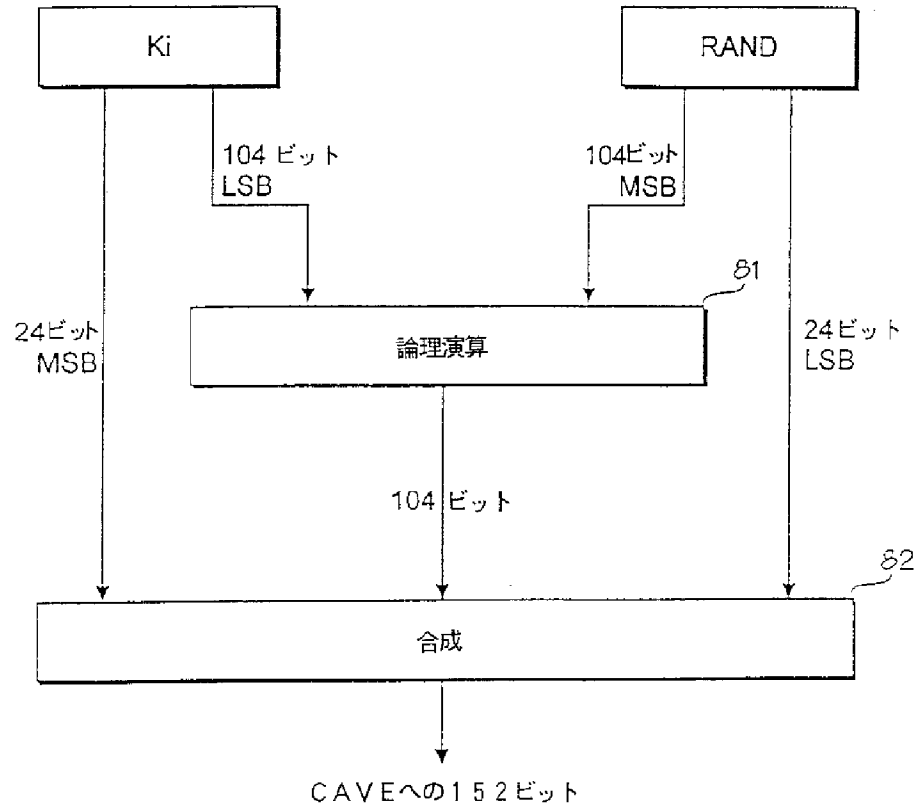
【図７】

Fig. 7


78
移動装置
確証結果(SRES)
確証要求 (RAND)
75
Ki
RAND
RAND
128 ビット
72
裁断
Ki 128ビット
TRAND
24 ビット
73
合成
COMB
152 ビット
77
76
A8
CAVE
18 ビット
74
パッド
14 ビット
32 ビット
Kc
SRES 32 ビット

【図８】

Fig. 8


Ki
RAND
104 ビット
LSB
104ビット
MSB
81
24ビット
MSB
論理演算
24ビット
LSB
104 ビット
82
合成
CAVEへの152ビット

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 96/00543

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/38, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0675615 A1 (FRANCE TELECOM), 4 October 1995 (04.10.95), abstract ---	1-8
A	US 5319710 A (M. ATALLA ET AL), 7 June 1994 (07.06.94), column 2, line 49 - column 6, line 16 --	1-8
P,A	US 5513245 A (S.MIZIKOVSKY ET AL.), 30 April 1996 (30.04.96), column 3, line 46 - column 4, line 26 -- ---	1-8

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 March 1997	20 -03- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Christina Halldin Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

03/02/97

International application No.
PCT/FI 96/00543

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0675615	04/10/95	FR-A,B- 2718312	06/10/95
		JP-A- 8008899	12/01/96
US-A- 5319710	07/06/94	AU-A- 664823	07/12/95
		EP-A- 0678836	25/10/95
US-A- 5513245	30/04/96	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国　　EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN